FORTINET
High Performance Network Security

FortiWLM

Release 8.4.0

Product Overview

The FortiWLM Application Suite is an intelligent management system that helps you to easily manage your wireless network. It shares a common administrator interface, making it easy to transition between the following applications:

- *FortiWLM (NM)*—is a web based application suite which manages controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network.
- *Service Assurance Manager (SAM)*—provides trouble-prevention capability that uses the FortiWLM infrastructure to perform end-to-end system tests, either on-demand or automatically at periodic configured intervals. SAM works by comparing a well-functioning network baseline metric to periodic tests. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with Service Assurance Manager.
- *Spectrum Manager (SM)*—is used to manage your network health. The SM uses a network of devoted sensors or one of the radios on non-dedicated Fortinet Access Points, to continually scan the environment for interferences. With Fortinet Spectrum Manager, you can identify sources of potential interference and present interferer data on graphical dashboards to deliver high bandwidth and control the wireless spectrum for high quality of service (QoS). The software based sensors detects and classifies sources of wireless interference and pro-actively manages channel interference issues. The sources for potential interference in 2.4 GHz and 5 GHz spectrum is identified and graphically represented on the dashboard.
- *Wireless Intrusions Prevention System (WIPS)*—Fortinet's WIPS provides complete wireless threat detection and mitigation into the wireless network infrastructure. It detects wireless intrusions using predefined and custom signatures on an integrated platform with other WLAN management applications.
  For more information, see the *Wireless Intrusion Prevention System (WIPS) User Guide*.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Product Documentation

This release of FortiWLM delivers a comprehensive set of customer documentation:

- Online Help integrated into the FortiWLM application. The online help provides detailed feature usage for this release.
- User Guide released and made available for detailed configuration and management of the FortiWLM 8.4.0.

What's New

This release of FortiWLM introduces the following new features and functionalities:

NOTE:
From this release, virtual FortiWLM installation supports 64-bit OS only, FortiWLM hardware models' (100D and 1000D) installation supports both 32-bit and 64-bit OS.

The forthcoming new FortiWLM hardware models will also support 64-bit OS only. Fortinet will issue the required notifications for the new hardware as and when they are available.

Migrating from Virtual FortiWLM 32-bit to Virtual FortiWLM 64-bit

This section describes the procedure to migrate data from virtual FortiWLM 32-bit to virtual FortiWLM 64-bit.

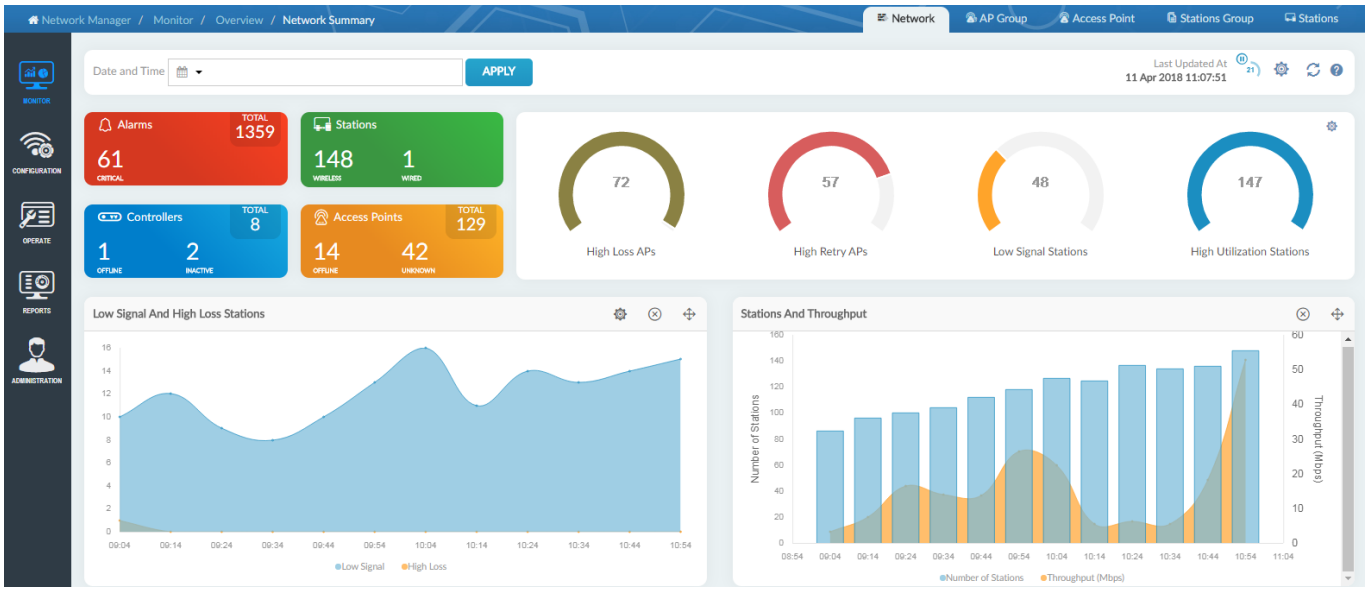
1. Backup the data in 32-bit FortiWLM and copy it using the copy scp/ftp command.
2. Install the 64-bit FortiWLM image.
3. Shutdown the 32-bit WLM instance.
4. Run the following commands in the 64-bit FortiWLM to copy and restore the backed up 32-bit data:
   - ***copy scp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.***
     OR
     copy ftp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.
   - ***restore <Backup file name>***

NOTE:

- Migration from SA2000-VE to FWM-VM 64-bit requires a new license file to be installed on FWM-VM 64-bit. For licensing options contact the *Sales Account team*.
- Migration from FWM-VM 32-bit to FWM-VM 64-bit does NOT require any license changes and you can continue to use the FWM-VM 64-bit setup.

User Interface enhancements

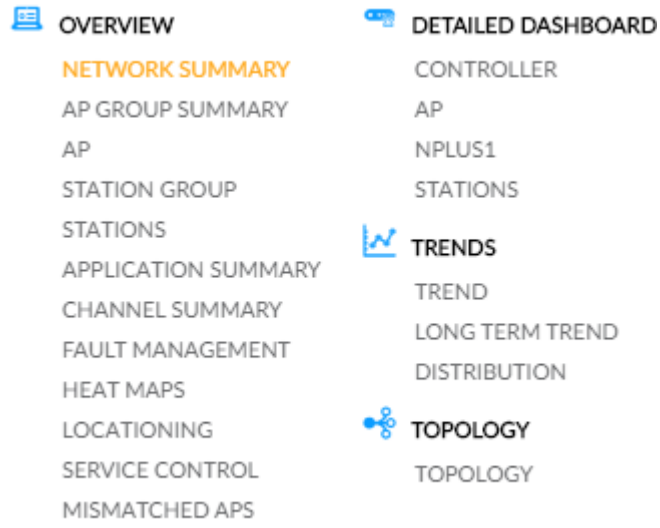
This release introduces a new user interface design to improve the FortiWLM accessibility and usability experience. The enhanced visual design provides improved aesthetics and look-and-feel to the user. The user interface is reorganized to provide the features and functionalities in a distinctive way so as to help the user find information without much browsing and also to ease navigation. The new user interface makes the FortiWLM more interactive and easier for the user to monitor and manage the elements in their network.



The user interface is segregated into five buckets.

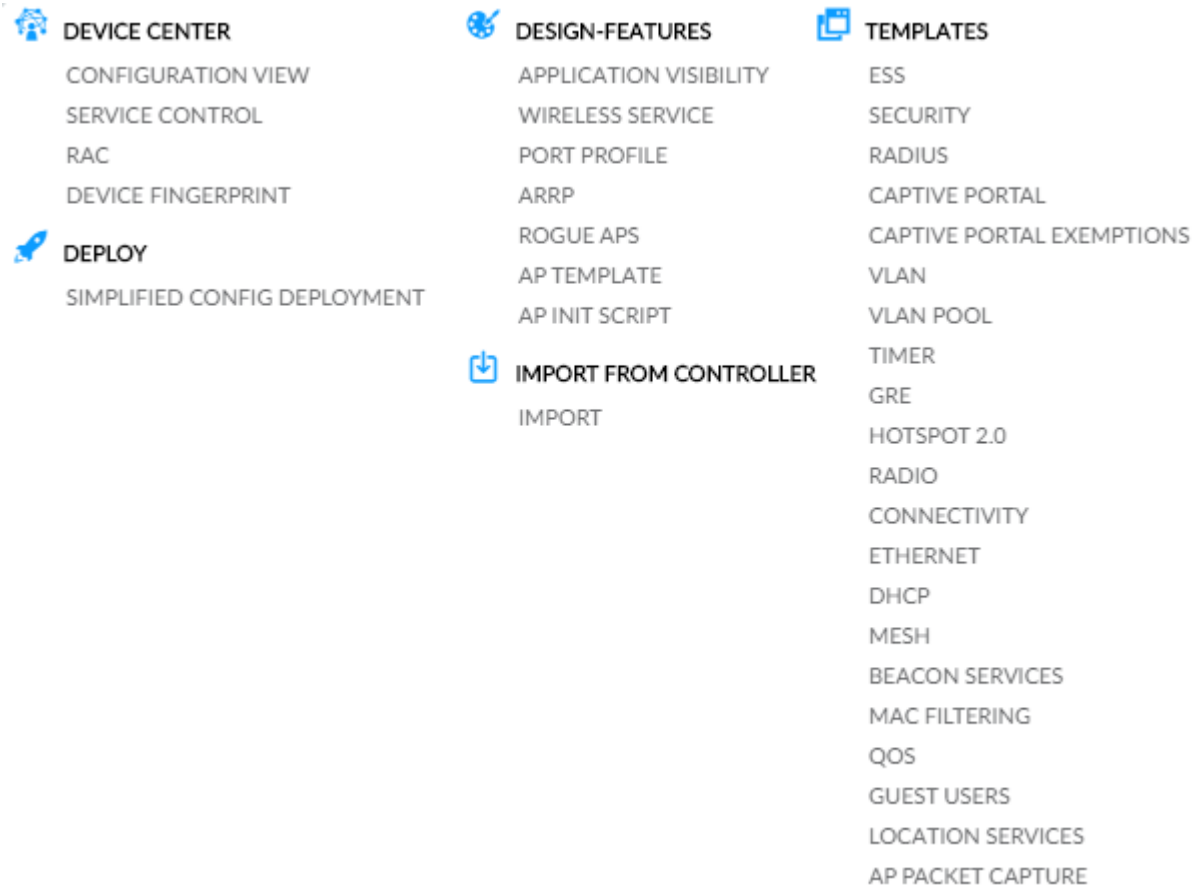
Monitor

The Monitor dashboards provide a summary view of all WLAN statistics. The graphical representation of Alarms, Controllers, Access Points, Stations, and Station by OS type provides a glimpse of the wireless network, based on the current and historical data stored in the database.



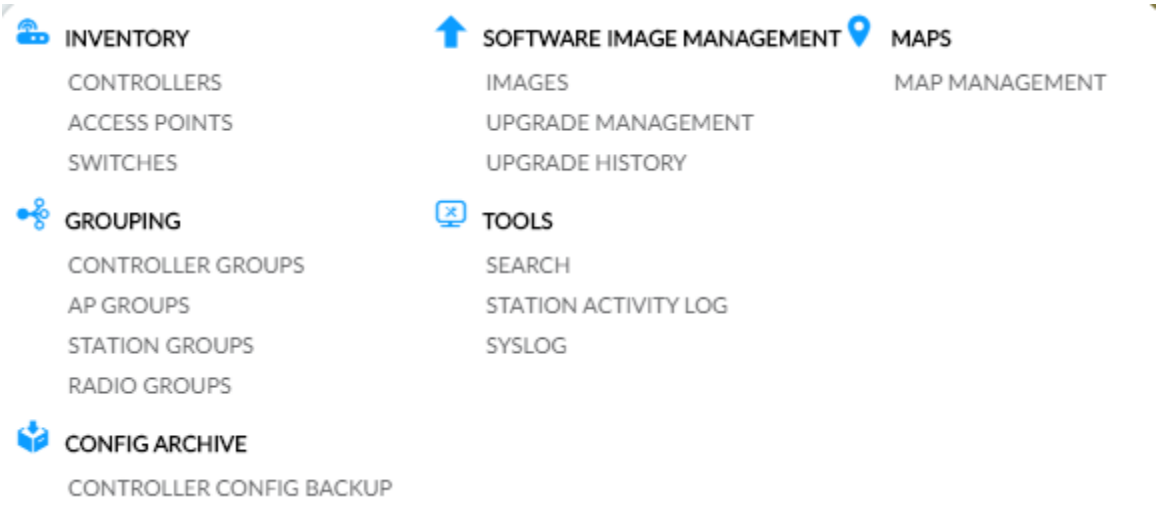
Configuration

The configuration menu allows you to configure and manage multiple controllers, access points, and stations. You can create common configuration and apply it to multiple devices in your network. These configurations are owned by the NMS – server.



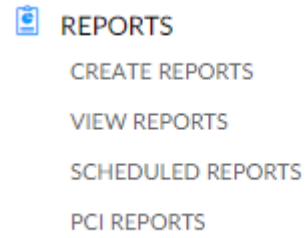
Operate

The operate menu allows you to monitor and manage the inventories in your network. You can add and delete controllers, access points, and switches. Group controllers, access points, stations, and radios for configuration purpose, and manage the software image installed.



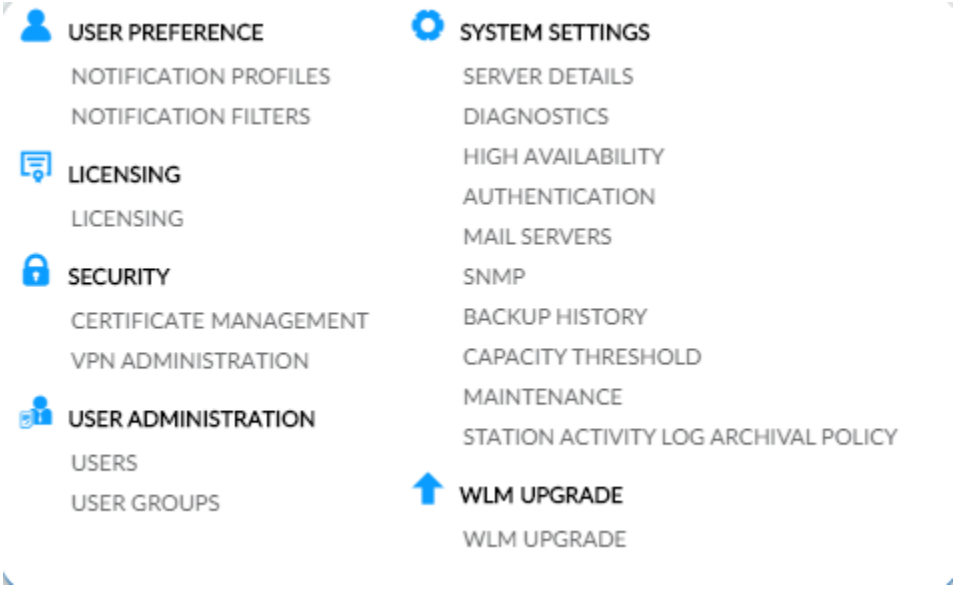
Reports

FortiWLM provides standard report types that assist you to generate, schedule and view reports. You can create and customize report types and save them as templates for future generation. Reports allow you to perform network analysis, user configuration, device optimization, and network monitoring on multiple levels. These reports provide an interface for multiple configurations, allowing you to act upon information in the reports.



Administration

The administration menu allows you to administer the users and devices in your network. You can manage the various system settings and upgrade FortiWLM.



Dashboards

This release of FortiWLM introduces new customizable dashboards that allow you to choose the statistics you want to view. These dashboards allow you to monitor the overall network health and also the performance of various elements in your network, such as controllers, access points, and stations; by providing a graphical representation of the performance of these devices within the administrative scope of the logged in user.

The dashboard filtering options allow you to refine the results displayed on the dashboard panels. The monitoring parameters of these interactive dashboards analyse the statistics and behaviour of specific devices and allow you to configure thresholds based on which the dashboards are plotted. The resizable dashlets on the various dashboards provide graphical and detailed insights into the selected performance parameters.

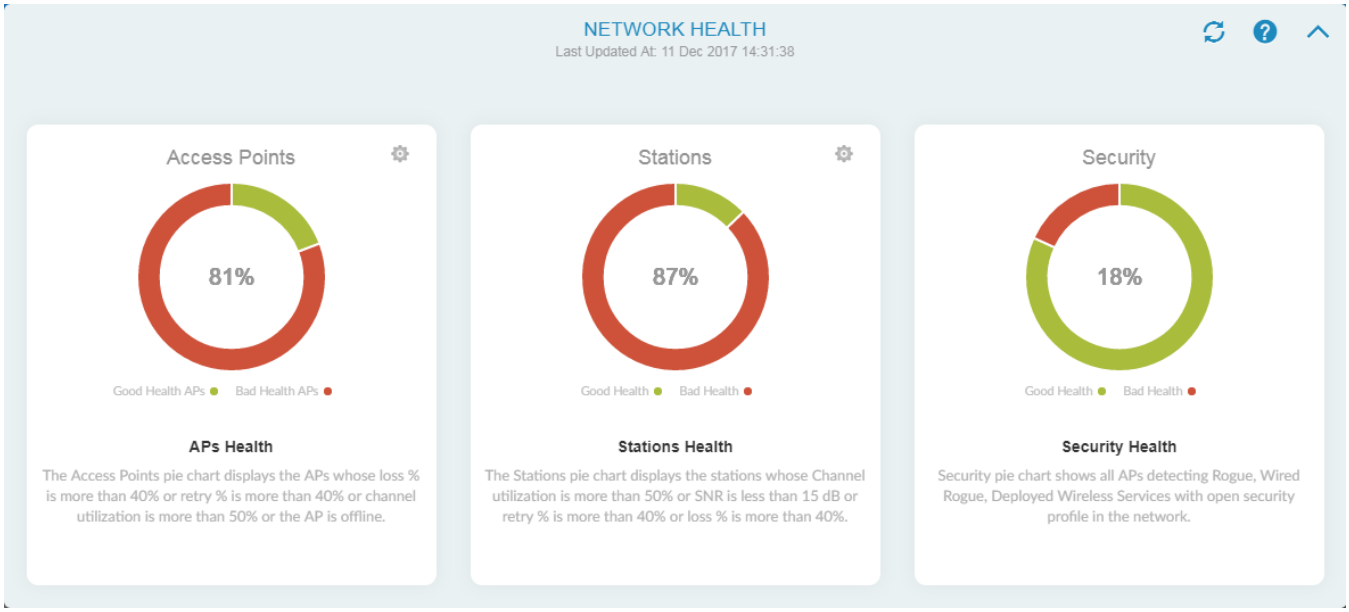
Navigate to **Monitor > Overview** to access the following new dashboards:

- Network Health
- Network
- AP Group
- Access Point
- Stations
- Stations Group

For detailed information on these dashboards, see the ***Online Help*** on the FortiWLM user interface.

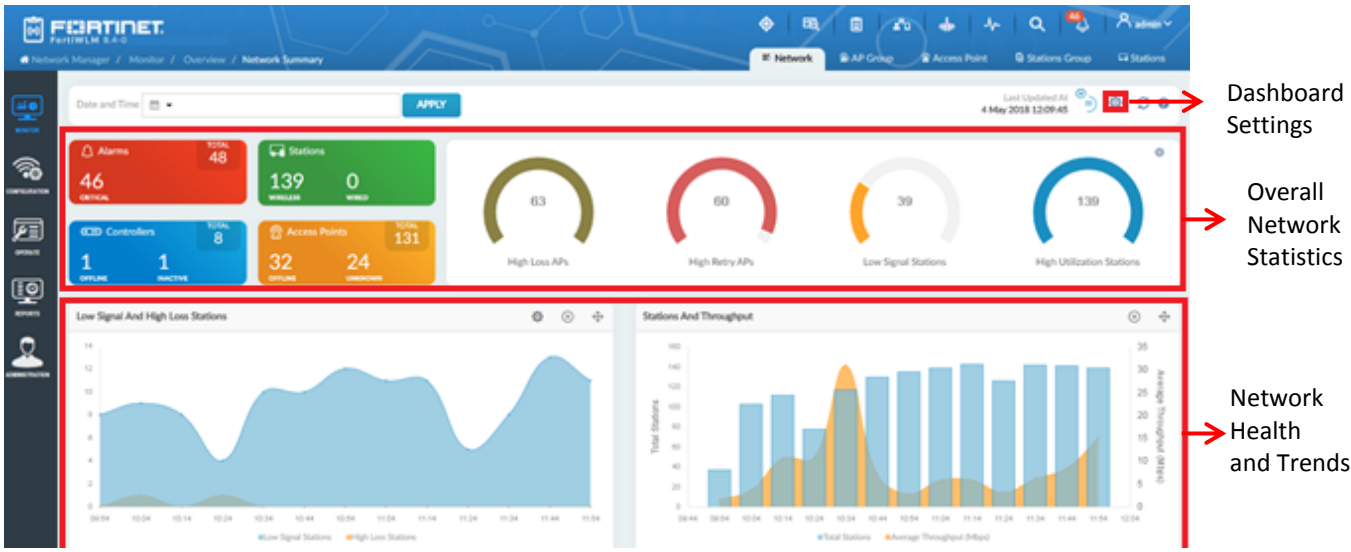
Network Health

The Network Health Dashboard monitors the devices in your wireless network and provides a health summary of the devices. The pie charts in this dashboard highlight the problematic devices/areas in the network by examining the statistics and behavior of stations and access points. You can identify the potential issues in the network using the data in this dashboard.



Network

The **Network** dashboard gives statistics of the type of devices connected to the network and their performance. It provides a summary view of WLAN statistics, including network wide wireless controller and access point performance distribution. It gathers the data from all managed controllers and access points at specific intervals. The graphical representation of Controllers, Access Points, Stations, and Station by OS type provides a glimpse of the wireless network, based on the data that is fetched for the configured period of time.

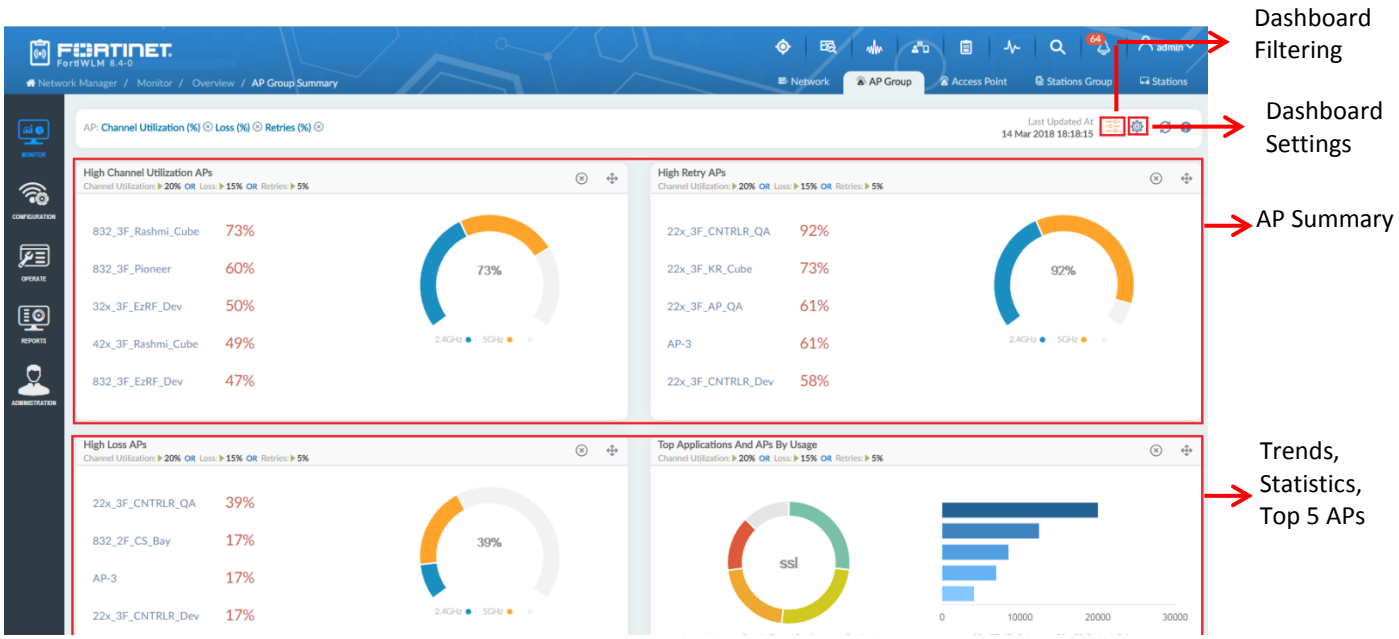


AP Group

An **AP Group** is a coherent group of APs belonging to the same controller or different controllers placed in distinctive geographic locations. The AP group may consist of APs with different hardware model or APs from controllers having different FortiWLC versions. When an AP is added to a group, all the radios of the AP are also a part of this group.

The APs data within the selected AP group is used to create the AP Group dashboard. The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes for other widgets) on the server. All the links or pop-up from this page and status bar display the current data.

The AP Group Summary dashboard provides data from Trends, Statistics, and Top 5 APs.

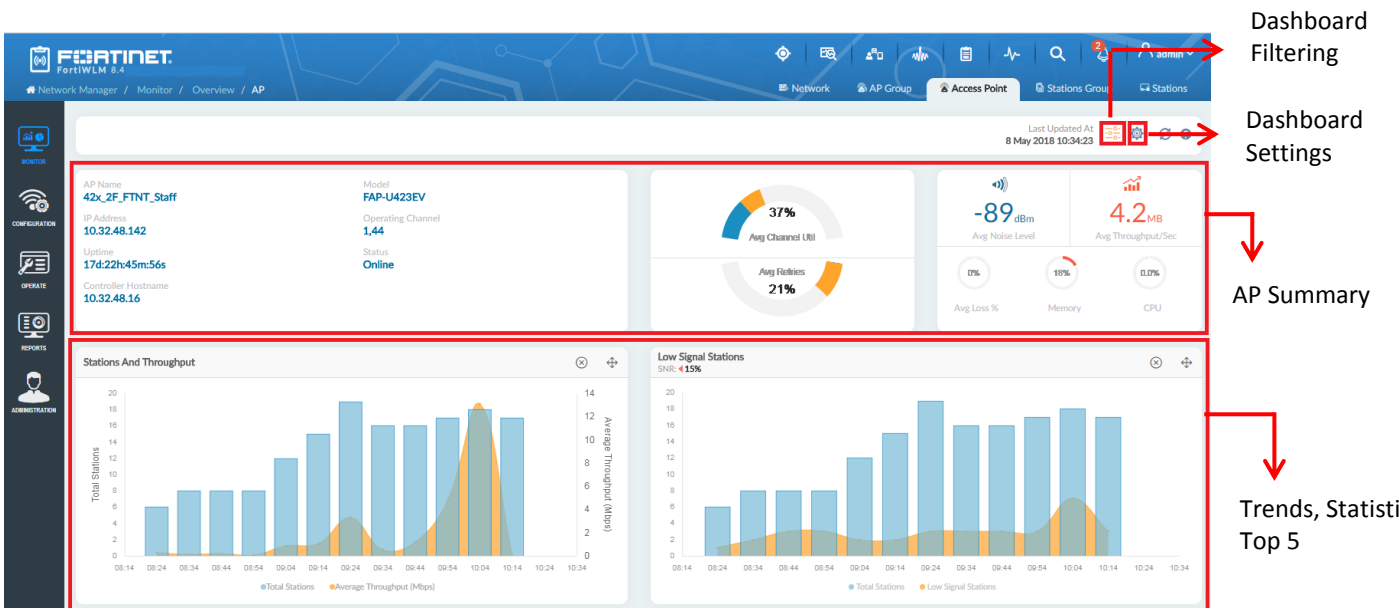


Access Point

The **Access Point** Dashboard screen displays in-depth information about the AP activity. It provides the graphical representation of the Throughput, Station Count, Noise Level, Loss%, Channel Utilization%, and the health of stations connected to the selected access point which is connected to a controller managed by the FortiWLM. The trend result for each of the stations of the selected AP is displayed on the top portion of the window.

The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes for other widgets) on the server. All the links or pop-up from this page and status bar display the current data.

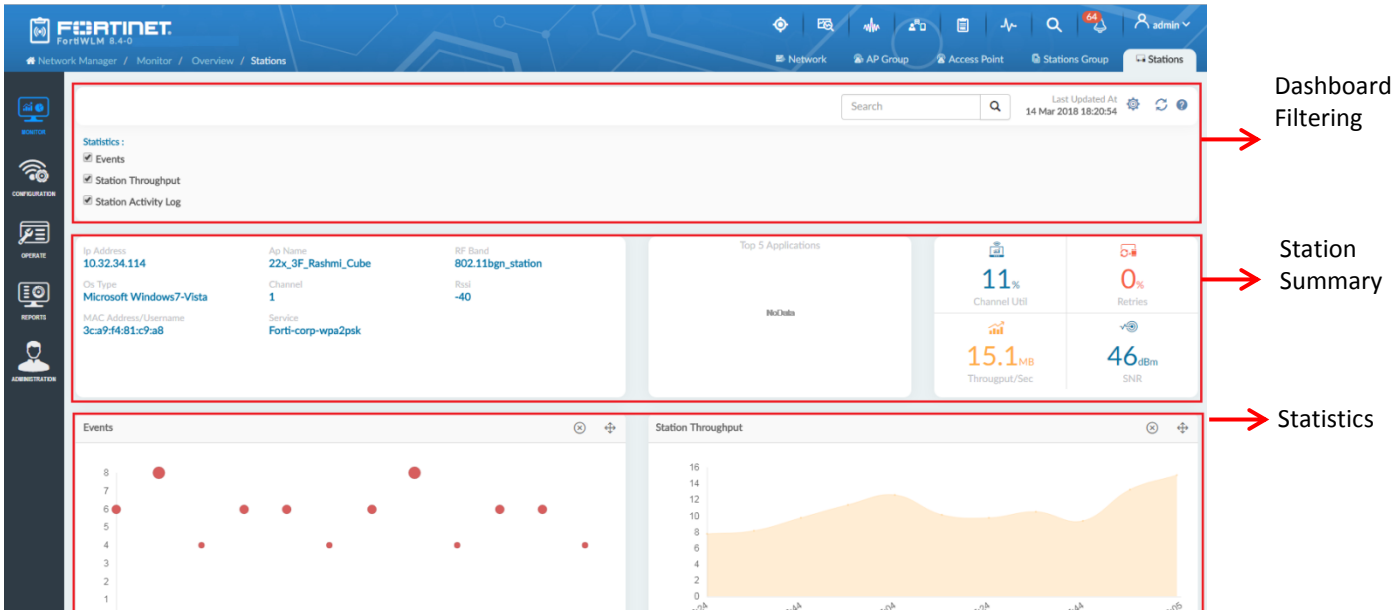
The AP Group Summary dashboard provides data from Trends, Statistics, and Top 5 APs.



Stations

The **Stations** Dashboard screen displays in-depth information about the station activity. It provides the graphical representation of the Throughput, events, and the health of stations connected to the access points which are connected to a controller managed by the FortiWLM.

The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes for other widgets) on the server. All the links or pop-up from this page and status bar display the current data.

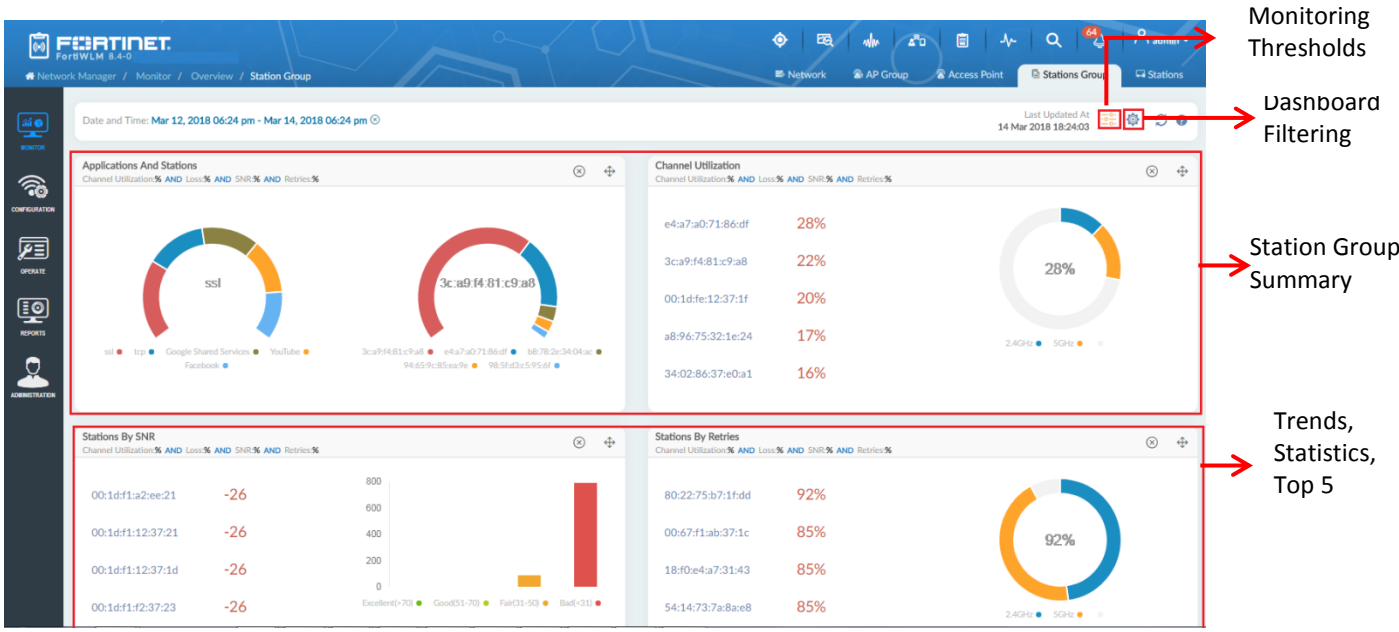


Stations Group

This **Stations Group** dashboard screen displays the summary of all the stations within the station group. This dashboard provides status, activity, and health details of all stations in a station group.
The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets

and 10 minutes for other widgets) on the server. Every station on the entire dashboard is clickable which will navigate to station dashboard for the particular station.

The Station Group Summary dashboard provides data from Trends, Statistics, and Top 5 Stations.



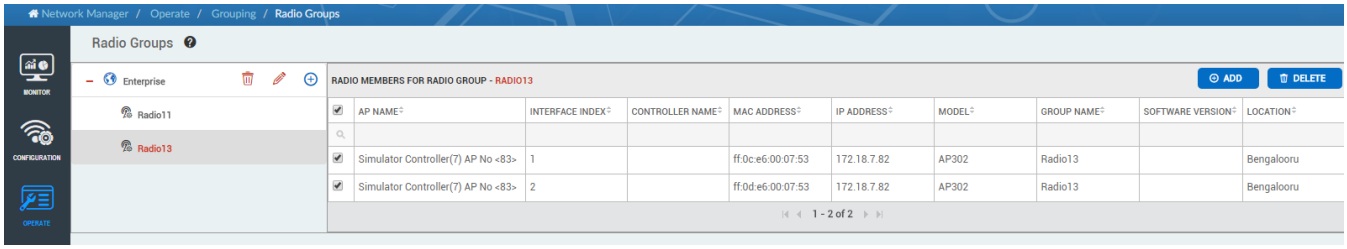
Radio Grouping

A Radio group is a static logical group of AP radios across controllers. Radio groups are used for monitoring and configuration purposes. A Radio can belong to multiple Radio groups.
You can deploy wireless services on particular Radios of the AP by selecting the Radio groups created. When deployed, services are deployed only on the AP Radios which are part of the Radio group.

When a new member is added to the Radio group, all the services deployed on the group are deployed on the new member as well.
When an AP or controller is deleted, corresponding radios of APs/Controllers are deleted from radio groups.

You can create multiple sub groups within a Radio group. FortiWLM provides an hierarchical representation of the radio groups and sub groups. Hover the mouse over the Radio group to view the name, time of the last update, and owner.

Navigate to **Operate > Grouping > Radio Groups.**



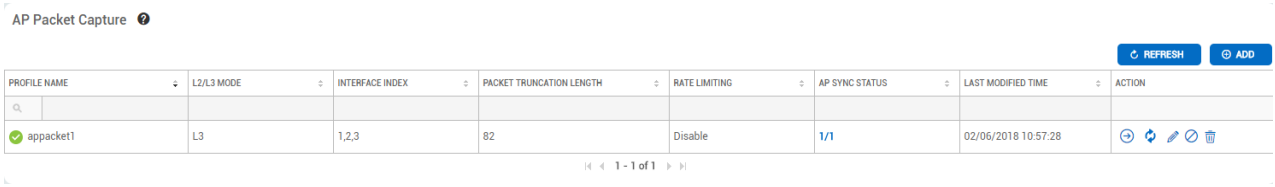
You can add, edit, and delete a Radio Group and add members to an existing Radio Group. For detailed information on various operations for Radio grouping, see the ***Online Help*** on the FortiWLM user interface.

AP Packet Capture

The FortiWLM supports packet sniffing from access points to handle wireless network security issues and forward the capture packet dumps to any required destination IP and Port.

You can capture packets over the air from access points while the AP continues to operate normally. Once packets are captured, you can see packet captures in real time or save them to a file for offline analysis. AP packet capture can be used when WIPS is configured on the access points for intrusion detection/prevention. You can forward packet captures from APs directly to external devices without storing packets locally on the controller. This eliminates the restriction on the file size of the packet capture (you are not limited by controller memory) and also allows the captured information to be stored and archived externally.
Use the FortiWLM to configure packet capture profiles to start or stop packet capture for clients.

Navigate to **Configuration > Templates > AP Packet Capture**.



You can add, edit, and delete an AP Packet Capture profile and apply it to AP groups or to specific APs of controllers. For detailed information on various operations for AP packet capture, see the ***Online Help*** on the FortiWLM user interface.

Location Services

The location service captures parameters at pre-defined intervals and sends them as UDP packets to your location engine to locate the position of a client / station in your network.

For non-wave2 APs, you will need Bluetooth adapters (for example: *Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Buletooth Dongle, Iogear Bluetooth 4.0 USB Micro Adapter GBU521*). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

NOTE: Access points must be connected to 802.3at power supply.

Navigate to **Configuration > Templates > Location Services**.

A default Location Services profile, *WLM_Locationing*, exists in FortiWLM with this configuration. You can enable and use the default profile.

- Report Format – Forti-Presence
- Project Name – FWLM
- Secret – The secret key displayed in *Administration > System Settings > Maintenance*.

Note:
In a HA setup, by default the primary server IP address is configured as the **Server IP Address.** Modify this to the VRRP IP address before enabling the default profile.

Fortinet recommends that you create a **new** location services profile with the following configuration:

- Location Services Feed: **Enable**
- Report Format: **Forti-Presence**
- Project Name: **FWLM**
- Secret: The secret key displayed in **Administration > System Settings > Maintenance.**
- Source Type: **ALL** or **WIFI**
- Server IP Address: FortiWLM IP address (VRRP IP address in case of HA)
- Server Port: **4013**
- Report Interval: **10**

Notes:

- For any modifications to the location services profile to be pushed successfully to the controller, disable and enable the modified profile.
- Only **Forti-Presence** report format is supported.

You can add, edit, and delete a Location Services profile and apply it to specific controllers. For detailed information on various operations for Location service profile, see the ***Online Help*** on the FortiWLM user interface.

Locationing

The locationing feature plots the current location of all stations on the floor map imported into the FortiWLM. FortiWLM plots the current location based on the location feed received from all controllers (which are in turn connected to APs) and does not display the movement of the stations.

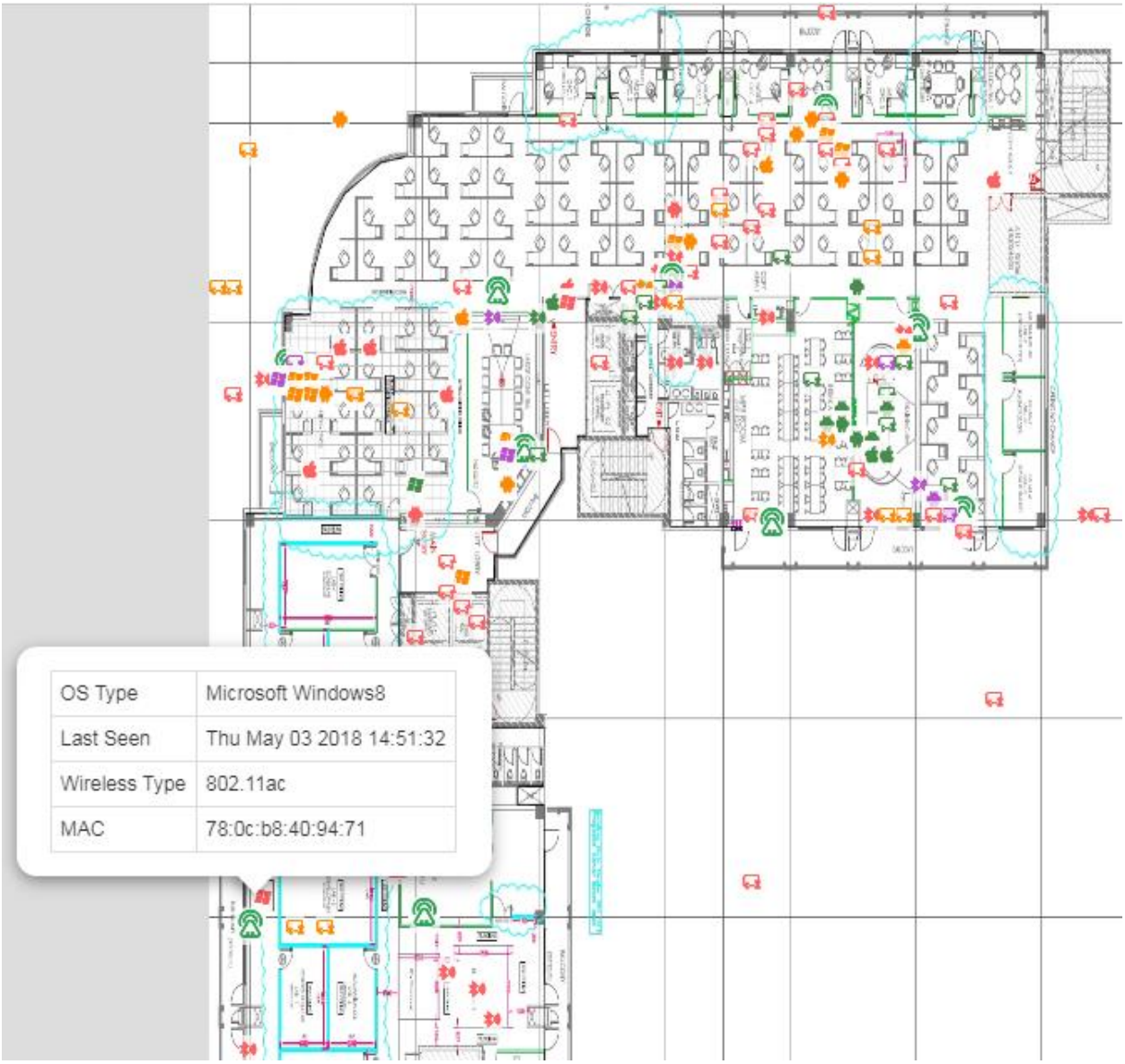
For FortiWLM to display the location data, a Location Services profile with the following configuration should be pushed to the controller. A default Location Services profile, *WLM_Locationing*, exists in FortiWLM with this configuration. You can enable and use the default profile.

- Report Format – Forti-Presence
- Project Name – FWLM
- Secret – The secret key displayed in *Administration > System Settings > Maintenance*.

Select the campus and the floor details to monitor the station locations. These filters can be applied, *Device Type, Wireless Type, OS Type*, and *Station MAC*. You can set the **Floor Visibility** and magnify the floor view.

Navigate to **Monitor > Overview > Locationing.**

For detailed information on locationing, see the ***Online Help*** on the FortiWLM user interface.



FortiSwitch Support

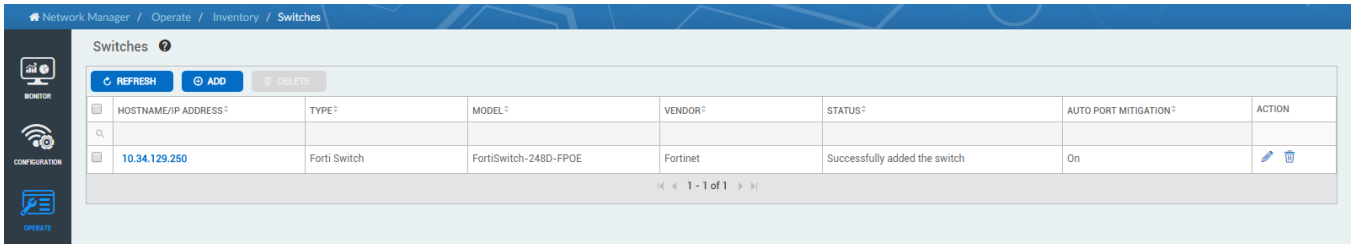
Switches use the SNMP protocol for fault management and REST for configuration and statistics.

- The FortiSwitch uses SNMP and REST credentials for detecting the wired rogues.
- Third party switches use only SNMP credentials for detecting wired rogues.

When using FortiSwitch, you can enable **Auto Port Mitigation** to block the port for AP mitigation when WLM detects a rouge AP connected to the FortiSwitch.

Navigate to **Operate > Inventory > Switches.**

For detailed information on FortiSwitch, see the ***Online Help*** on the FortiWLM user interface.



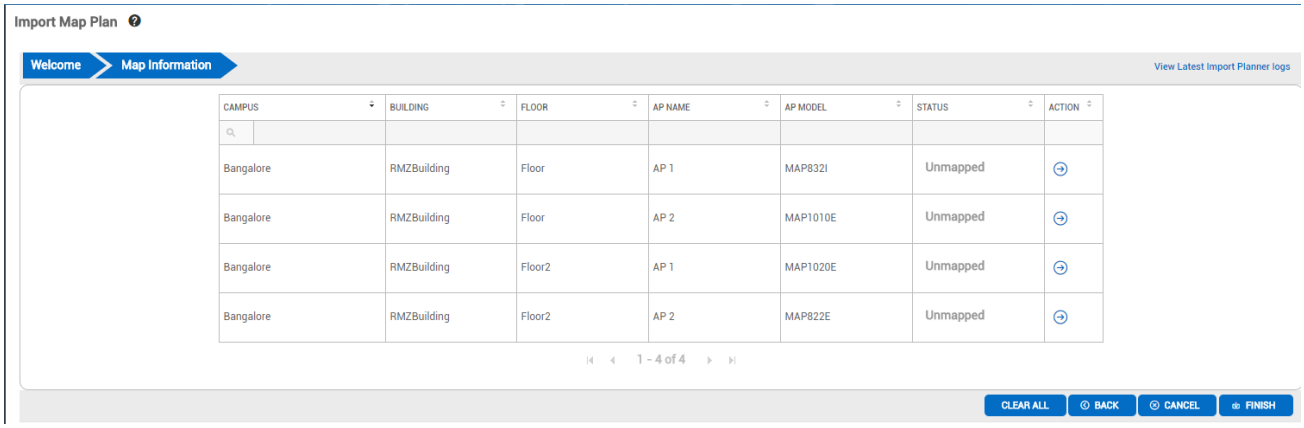
Importing from FortiPlanner

FotiWLM supports importing a floor map plan created on and exported from the FortiPlanner. Once the floor plan is created in the FortiPlanner, select **Export** in the project menu. The floor map to be imported is a *.zip* file.

Note:
Only exported *.zip* files from the FortiPlanner can be imported. Contact the Customer Support to obtain the relevant FortiPlanner version.

For more information on creating floor plans on the FortiPlanner, see the *FortiPlanner User Guide*.

Navigate to **Operate > Maps > Map Management > Import.** Browse to *.zip* file and click **Import**. Map the unmapped APs as required and click **Finish**.



You can add or delete APs from the floor map. For detailed information on importing the Forti-Planner, see the ***Online Help*** on the FortiWLM user interface.

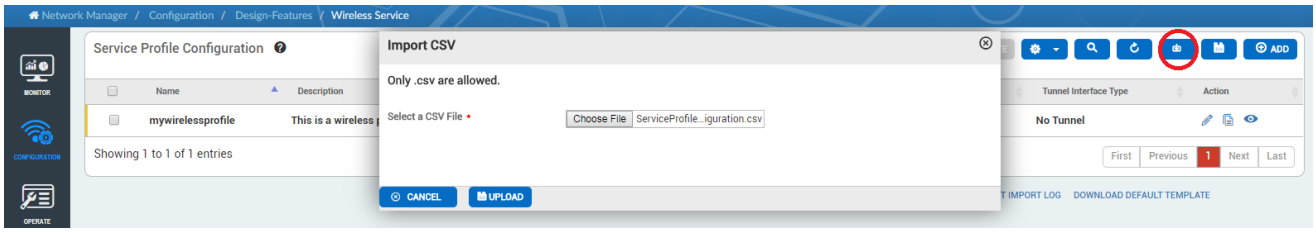
IPv6 address for Stations

FortiWLM supports assigning IPv6 address to the stations in your network. Navigate to **Monitor > Topology** to view the station IPv4/IPv6 address.

Import of Wireless Profiles

FortiWLM supports importing a Service Profile (*.csv) from your local drive and uploading it to FortiWLM.

Navigate to **Configuration > Design-Features > Wireless Service**.



Virtual FortiWLM 64-bit only

The virtual FortiWLM is now released as a 64-bit image only. For more information on migrating from an older 32-bit virtual FortiWLM to an 8.4.0 64-bit FortiWLM, see Migrating from Virtual FortiWLM 32-bit to Virtual FortiWLM 64-bit.

Data Indexing

After upgrade to FortiWLM 8.4.0 or after performing data backup and restore, partition (aggregation) tables are created in the database. Data indexing process symbol is displayed in the GUI. There might be a discrepancy in the older data displayed on the dashboards.

Enhancements

In **Administration > System Settings > Authentication,** multiple authentication modes (Local, Radius and TACACS+) can be enabled at a time and authentication to the FortiWLM server can be done using any of the enabled authentication modes. The order of authentication when all three modes are enabled is Local, Radius and then TACACS+.

Additional Information

This section describes information related to the usage of FortiWLM.
The GUI menu option (*Administration > System Settings > High Availability*) to configure high availability from has been removed for FortiWLM-100D and SA250 platforms.

Supported Security Modes

This table lists the security modes supported for the Service Assurance Manager (SAM) on FortiWLM.

AP Models	Security Modes Supported	Security Modes Not Supported
All supported models	Open	WPA2 PSK TKIP
	WPA2 Enterprise AES	WPA2 Enterprise TKIP
	WPA2 PSK AES	WEP64
	Mixed PSK TKIP	WEP128
	Mixed Enterprise TKIP	SMS4

Fixed Issues

These issues are fixed in this release of FortiWLM.

Bug ID	Description
353022	EZRF not responding to all SNMP queries.
446443	AP reboots while upgrade performed on FortiWLM.
448210	Local and TACACS+ users are not able to view all tabs on the FortiWLM after upgrade to 8.3-2. It works fine for admin user.
455203	Session Timeout - Does not extend on non-admin accounts.
437219	FortiWLM Controller statistics missing on FortiWLC 3000D controller.
370758	Rouge AP alarms even if Rouge Detect is disabled on controller side.
458971	*Enhancement*: Increase size of maps on screen in Map Management.
446769	Configuration manager trying to sync profiles in a loop which made the FortiWLM unreachable.
422512	Unknown APs should not be considered as part of license consumption.
402445	FortiWLM tracks and reports history of configuration changes, but does not report the User/Admin that changed it.

Known Issues

These are the known issues in this release of FortiWLM.

Bug ID	Description	Impact	Workaround
467715	L2 error observed for SAM baseline tests with WPA2 PSK TKIP, WPA2 Enterprise TKIP, WEP64, WEP128, SMS4.	Station authentication fails.	Use other Security modes for running SAM tests.
473689	When upgrading from FortiWLM 8.3.3 to 8.4.0 via GUI on the non-default port, the upgrade page gets irresponsive.	The GUI upgrade page does not display the upgrade status.	Use the CLI mode to upgrade.
473226	WLM upgrade from 8.3.1 to 8.4 is failing.	Upgrade cannot be performed.	Contact the Customer Support for installing the relevant patch.
465837	Not able to upload 8.4 WLM upgrade (tar) file from GUI of 8.3.1 WLM.	Upgrade cannot be performed.	
455957	Upgrade Module command support required on WLC which is causing nmsagent installation failure from WLM.		
476199	VPN server IP and port number configuration lost after slave FortiWLC reboot in VPN Nplus1 setup.	VPN client status shows disconnected and not able to establish the tunnel between FortiWLC and FortiWLM.	Reconfigure the VPN client in FortiWLC to re-establish the tunnel between FortiWLC and FortiWLM.
472501	Spectrum Manager dashboard page is not displayed in the Microsoft Edge browser.	The Spectrum Manager dashboard page does not load.	Apply self-signed or third party trusted certificate on FortiWLM. Enable flash on Microsoft Edge browser.
484999	The upgrade GUI screen gives an incorrect “Failed to Restart Service” error message when the database is huge.	User receives incorrect error message.	Contact the Customer Support for installing the relevant patch.
488596	Station RF and Channel Distribution report taking long time to generate.	• The Station RF and Channel Distribution report for 1 day takes approximately 1 hour. • Station RF and Channel Distribution report for 1 month takes approximately 6 hours.	

Upgrading FortiWLM

This section describes procedures for upgrading your Services Appliance.

Pre-requisites

- To discover the FortiWLC 8.3.3 64-bit controllers (**listed below**) in FortiWLM 8.4.0, you need to apply the FortiWLC 8.3.3 patch. Contact the Customer Support for installing the relevant patch.

  - FortiWLC-1000D
  - FortiWLC-3000D
  - FWC-VM-50
  - FWC-VM-200
  - FWC-VM-500
  - FWC-VM-1000
  - FWC-VM-3000

- Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade. While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported FortiWLM Upgrades

The following upgrade path is recommended.

From FortiWLM version…	To FortiWLM version
6.1-3-6/7.0-5-0	8.0-7-0
6.1-3-6/7.0-5-0/8.0-7-0	8.0-SR1-1
8.0-7-0/8.0-SR1-1	8.1-2-0
7.0-5-0/8.0-7-0/8.1-2-0	8.2.2
8.1-2-0/8.2.2	8.2.4
8.1-2-0/8.2.2	8.3.0
8.2.4/8.3.0	8.3.1
8.2.4/8.3.0/8.3.1	8.3.2
8.2.4/8.3.1/8.3.2	8.3.3
8.3.1/8.3.3	8.4.0

Supported FortiWLC Releases

Network Manager Version	Supports Controllers with these FortiWLC-SD Versions
8.4.0	• 7.0-11MR-1 • 8.0-6-0 • 8.1-3-2 • 8.2.7MR-1 • 8.3.1 • 8.3.3 **Note:** [*FortiWLC 8.3.3 64-bit only*] – Contact Customer Support for installing the relevant patch. See bug 455957. • 8.4.0

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
Service Assurance Manager	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV

Hardware / Software	Supported Versions/Models
Spectrum Manager	• AP332 • AP832 • PSM3x • AP1010 • AP1020 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U221EV • FAP-U223EV • FAP-U24JEV • FAP-U422EV
Controller Models	• FortiWLC-200D • FortiWLC-500D • FortiWLC-50D • FortiWLC-1000D • FortiWLC-3000D • MC1550 • MC1550-VE • MC3200 • MC3200-VE • MC4200 • MC4200-VE • FWC-VM-50 • FWC-VM-200

	• FWC-VM-500 • FWC-VM-1000 • FWC-VM-3000
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • FWM-VM • Hyper-V (*supported only on Windows 2016 server*) • KVM *The following service appliances are **NOT** supported on 64-bit FortiWLM:* • SA250 • SA2000 • SA2000-VE • AEC200 • AEC2000
	# Due to hardware limitations, High Availability is not supported in FortiWLM 100D and SA250 appliances.
Supported Browsers	• Internet Explorer 9 and later version (*All the pages of EzRF will load under normal browser settings. Compatibility View Settings are not supported*.) • Mozilla Firefox 60.0 • Google Chrome, version 34.0.1847.118 m • Microsoft Edge (Windows 10) • Safari (MacOS) 11.0.3

Application Visibility Policies

Application visibility policies in controllers running FortiWLC-SD 8.0 that is managed by FortiWLM 8.1 or later will be disabled. To continue using those policies, upgrade FortiWLC-SD to 8.1 or later.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions prior to FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

Upgrading via CLI

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

```
sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

```
sa# sh flash
6.0-7-0 8.2-
1-0
```

7. Upgrade the service appliance:

```
sa# upgrade nms-server <Version>
```

This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.

8. Type the following command to confirm, if the installed software version is 8.3.3.

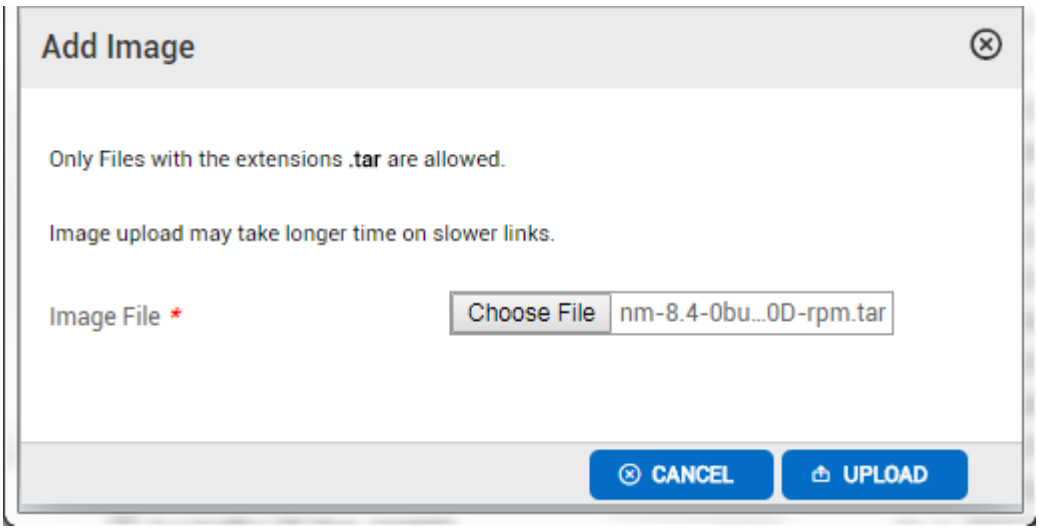
```
service appliance# sh nms
```

If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

Upgrading via WebUI

The following procedure will guide you through the steps to upgrade your server from WebUI.

1. In the Network Manager WebUI, go to **Administration > WLM Upgrade**. By default, this page lists all the images copied to the server.
2. To upgrade your server to a different version than the ones listed, click **Add** to open the file selector window.



3. Select the image file from your computer or a network folder and click the **UPLOAD** button
4. After the upload is complete, select the version to install and click the **INSTALL** button to being the upgrade process.

During the upgrade process, do not click refresh or perform any operations on the server.

After the upgrade is complete, click Go the link to return to server operations.

- For a full upgrade, the server will restart after the upgrade process and return the page to server login prompt.
- For patch upgrade, the server will restart the process and return to the dashboard.

Post Upgrade Tasks

The following are optional post-upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration > System Settings > Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrading FortiWLM

Downgrading FortiWLM to a previous version is not supported. To go back to an older version of FortiWLM, you must do a fresh install of that version on your FortiWLM server.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service